Kedos Srl
Information Technology Solutions

Emissione di certificati formativi digitali con garanzia di sicurezza e autenticità tramite blockchain

Caso d'uso 2023 - Blockchain

Introduzione

In questo progetto è stata sviluppata una soluzione software denominata KeCert, per l'emissione di certificati formativi (lauree, diplomi, attestati, ecc.) tramite l'utilizzo della tecnologia blockchain. Questa soluzione consente agli enti formativi (scuole, ITS, università, enti di formazione, aziende, ecc.) di rilasciare certificati digitali in pochi minuti garantendone la sicurezza e l'autenticità. L'utilizzo della tecnologia blockchain, che garantisce l'immutabilità delle informazioni in un registro condiviso, consente di certificare tutti i passi del processo, dalla emissione fino alla validazione, gestendo anche la possibilità di revocare i certificati. L'ITS ICT Piemonte è stato il primo partner che ha adottato la soluzione KeCert. L'esigenza principale dell'ITS piemontese era quella di rilasciare i certificati dei diplomi dei corsi biennali in tempi brevi, subito dopo il superamento dell'esame finale, garantendone l'autenticità e la condivisione immediata (es. su Linkedin).

La società partner

La Fondazione ITS ICT della Regione Piemonte rappresenta un'eccellenza nell'istruzione tecnica superiore, rispondendo alla crescente domanda di competenze avanzate nel settore tecnologico. Offriamo percorsi biennali post-diploma gratuiti, finanziati dall'Unione Europea, dal Ministero dell'Istruzione tramite il PNRR e dalla Regione Piemonte attraverso il PR FSE 21-27, formando tecnici superiori altamente specializzati e pronti a inserirsi nei settori chiave dell'economia. I percorsi, tra cui Digital Strategist, Full Stack Developer, Cyber Security Specialist e AR/VR and Game Developer, sono progettati con un forte orientamento al mondo del lavoro. Oltre il 50% dei docenti proviene dal settore professionale, garantendo una formazione aggiornata e pratica. Ogni percorso di 1.800 ore include 630 ore di tirocini obbligatori, sia in Italia che all'estero tramite Erasmus+, e attività pratiche in laboratorio. Dal 2023, grazie ai fondi PNRR, la Fondazione si è adoperata per la creaazione di nuove sedi e laboratori all'avanguardia in aree strategiche come Cyber SOC, AR/VR e DevSecOps. Questo impegno costante verso l'innovazione è riconosciuto da INDIRE, che la colloca ai vertici per le performance occupazionali e la qualità dei percorsi formativi. Il diploma di specializzazione tecnica superiore che rilasciamo, riconosciuto a livello nazionale e classificato al V° livello dell'EQF, prepara i giovani a una carriera di successo in un mondo tecnologicamente avanzato e in continua evoluzione.

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Lo standard Blockcerts

Per garantire l'utilizzo di un formato di certificazione delle competenze il più possibile standard e aperto è stato utilizzato il progetto open source Blockcerts, ideato e sviluppato dal MIT Media Lab.

Lo standard Blockcerts prevede l'emissione di certificati su blockchain tramite l'utilizzo di un formato JSON aperto. Blockcerts consente l'emissione in contemporanea di più certificati mediante una sola scrittura sul registro condiviso. Inoltre, nel formato è possibile inserire anche l'immagine del certificato, compresi i loghi dell'ente di certificazione ed eventuali firme. Questo rende il certificato facilmente condivisibile tramite il solo indirizzo del blocco nel registro (un esempio è riportato qui).

Durante lo sviluppo del progetto KeCert, il gruppo di ricerca e sviluppo di Kedos ha anche collaborato all'evoluzione del progetto Blockcerts con contributi sui codici sorgenti del progetto su github.

Il progetto

Come già accennato, l'obiettivo del progetto è supportare gli enti nella fase di emissione dei certificati formativi al termine di corsi o unità didattiche, e in tutte le fasi successive di gestione dei certificati, tramite l'immutabilità dei dati nella blockchain.

La soluzione consente agli enti formativi di produrre un certificato digitale che possa essere utilizzato dal beneficiario del corso per dimostrare le competenze e i titoli acquisiti garantendo al tempo stesso la sua autenticità e verificabilità.

KeCert utilizza la blockchain Ethereum, una delle blockchain pubbliche più utilizzate per lo sviluppo di applicazioni. Il servizio KeCert utilizza 4 fasi (Figura 1):

1. La creazione del certificato (tramite KeCert);
2. La creazione della transazione su Blockchain (tramite Blockcerts);
3. La scrittura del dato nel registro condiviso (tramite Ethereum);
4. L'emissione del certificato e del link di condivisione dello stesso (tramite KeCert).

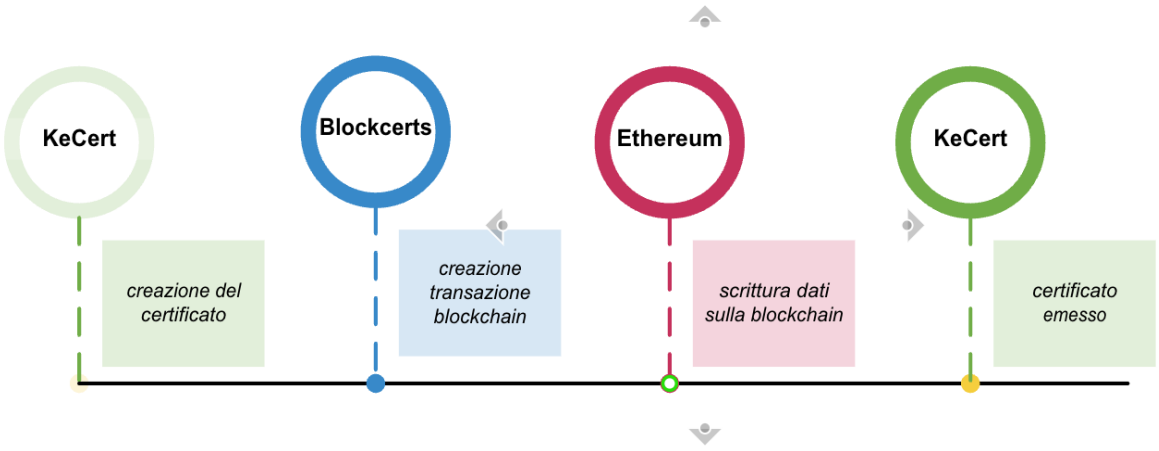

Figura 1: lo schema di emissione del certificato

I dati del certificato contengono tutte le informazioni come l'ente di formazione, il titolo del corso, la data di rilascio, ecc. L'identità dell'ente emittente è basata sull'utilizzo della crittografia a chiave

pubblica, con il deposito della chiave pubblica su un sito web ospitato su un dominio dell'ente di formazione, es. la pagina KeCert nel dominio dell'ITS ICT Piemonte e la chiave pubblica dell'ITS ICT Piemonte.

Una volta che il certificato è inserito all'interno della blockchain è possibile verificare in qualsiasi momento la sua autenticità con un *verifier* che estrae il JSON memorizzato all'interno della blockchain e lo verifica tramite la chiave pubblica del firmatario. L'architettura prevede anche un meccanismo di revoca del certificato per gestire eventuali anomalie emerse successivamente alla sua emissione (Figura 2).

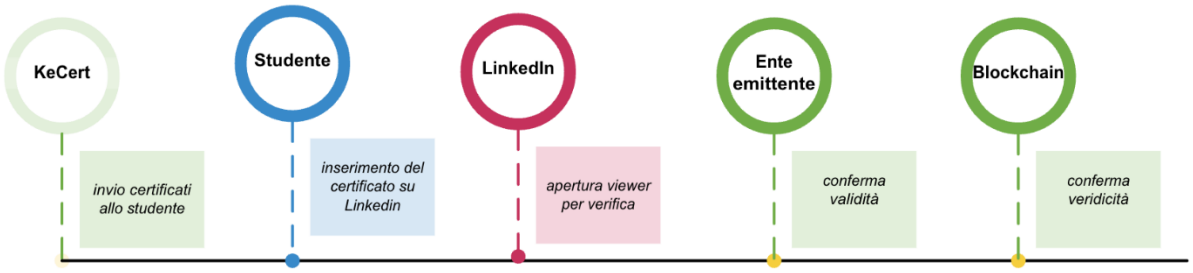

Figura 2: lo schema di utilizzo e validazione del certificato

L'architettura del progetto

La soluzione è composta da due parti distinte e connesse, la prima parte consiste nel software di backoffice per le agenzie formative, che possono inserire tutti i dati necessari per il certificato e procedere alla sua emissione e gestione (Figura 4). Per la creazione del certificato digitale con il software web di backoffice è possibile visionare questo video.

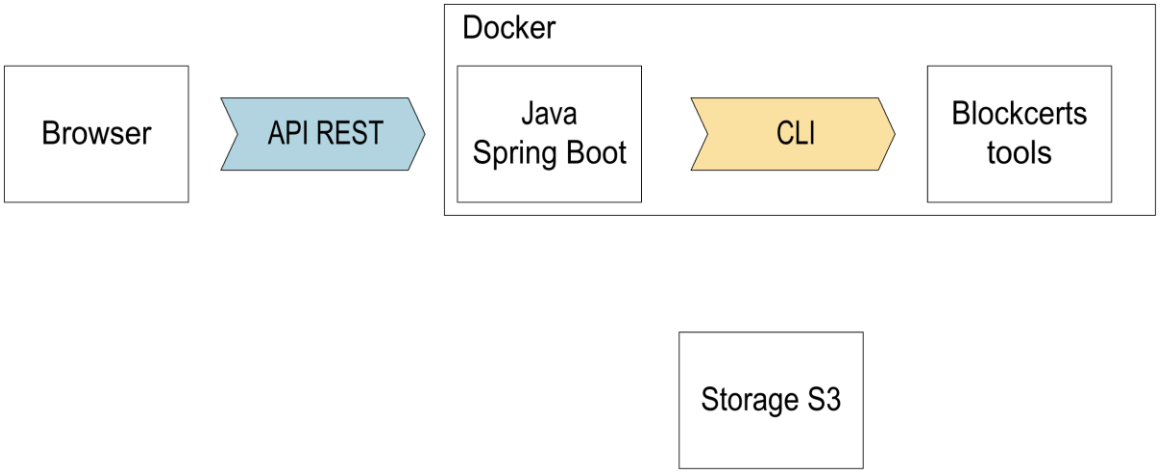

Figura 4: schema architetturale dell'area riservata

La seconda parte, disponibile pubblicamente online, consente di visualizzare il certificato in una forma grafica personalizzabile e avviare il processo di verifica (senza necessità di interpellare l'ente emittente).

La verifica avviene tramite l'utilizzo di un client in Javascript che controlla la firma sul certificato utilizzando la chiave pubblica dell'ente certificatore. Qui è riportato un esempio di certificato digitale rilasciato dall'ITS ICT Piemonte di Torino (Figura 5).

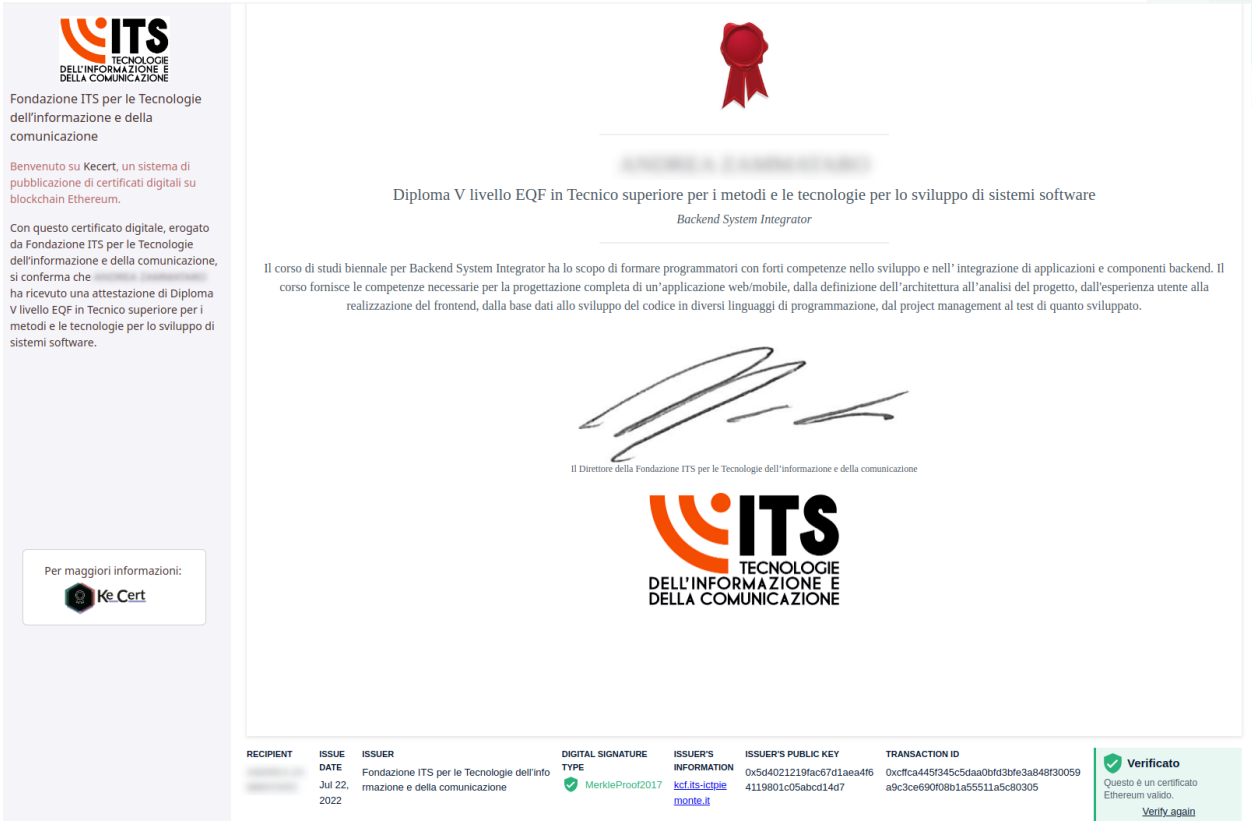

Figura 5: esempio di certificato digitale rilasciato con KeCert

Per offrire una soluzione architetturale aperta si è scelto di sviluppare uno strato di web API con un'architettura REST. Questo strato è stato sviluppato in Java. Lo sviluppo di questa interfaccia ha consentito un'integrazione agevole con i tool Blockcerts sottostanti. Per l'integrazione con la blockchain si è utilizzato il progetto Ethereum, una delle tecnologie blockchain più famose al mondo.

Utilizzando l'architettura REST è possibile integrare il progetto KeCert in software di terze parti tramite delle semplici connessioni HTTP, utilizzando un sistema di API key per l'autenticazione.

Conclusioni

In questo progetto è stata sviluppata una soluzione di gestione dei certificati formativi su blockchain.

La soluzione utilizza gli standard open Blockcerts e Ethereum per consentire la certificazione e la trasparenza delle informazioni su un registro pubblico distribuito.

La soluzione può essere estesa ad altri ambiti oltre a quello formativo, in ogni occasione in cui vi sia necessità di garantire la veridicità di certificare delle competenze.

Infine, per agevolare l'integrazione in applicativi esistenti è stato sviluppato uno strato di API REST interrogabile tramite protocollo HTTP. Questa soluzione consente una semplice integrazione con applicativi di terze parti, ad esempio in applicativi gestionali utilizzati da altre aziende in modalità Software as a Service (SaaS).

Kedos Srl

Kedos κῆδος

Kedos in greco antico significa Cura. L'impegno profuso per creare le migliori condizioni è il significato del nostro nome. Kedos è quindi il nostro manifesto d'intenzione nell'ambito di ogni progetto che ci vede coinvolti e di ogni proposta che portiamo sul mercato. La società offre servizi di consulenza IT e sviluppo soluzioni software in vari ambiti, utilizzando diverse tecnologie e metodologie. Negli ultimi anni l'azienda si è specializzata nell'utilizzo dell'Intelligenza Artificiale, delle tecnologie Blockchain e dei motori di Rendering 3D. All'interno dell'azienda è presente un dipartimento di Ricerca e Sviluppo che offre soluzioni innovative utilizzando le tecnologie di frontiera in ambito IT. La società ha sedi a Parma, Milano e Torino.